Chapter I

Executive Overview

Lawrence M. Oliva

The Ubiquitous New World of IT Security

The convergence of many interdependent events, including the expansion of unprotected Internet connected applications, the global war on international terrorism and the large financial impacts of information and identity theft, has made IT security a core element of most corporate and government IT plans. During 2003, two examples illustrate the scope and cost of the security problem: Cyber attacks increased 40% in the first three quarters of the year, and the cost of cleaning up multiple worm and virus attacks during the summer cost $3.5 billion, according to the CERT Coordination Center, a cyber security-monitoring agency.

Interwoven with capacity, performance and reliability factors, internal security strategies have expanded past keeping external hackers and crackers out to authenticating users through biometric and other factors, tracking authorized access inside firewalls by system users, and forensic analysis of destructive software. Given the economic con-
straints placed on business expenses, however, these efforts have often been too little, too late to stop determined individuals from gaining access to information assets.

Adding to the technical complexity of security are legal issues concerning user privacy, liability issues for not preventing the theft of customer records and identities, and government compliance with HIPAA, GLBA, FCRA, NORPDA, PIPEDA, SAFETY, Sarbanes-Oxley, and the U.S. Patriot Act regulations. Overlaying proactive long-term plans and operations are immediate reactive limitation activities to network and system-wide attacks caused by malicious software (also called “malware”) such as worms, viruses, Trojan horses and zombies.

As technology reliability has moved user expectations to a 24×7 availability level, the level of management complexity associated with that degree of service has required larger equipment investments, more staffing, and increased awareness of the consequences of each decision made concerning IT security. By default, IT managers and executives have been forced to become experts — with associated responsibilities — on many different topics outside the traditional IT community.

This added level of management complexity is just now being recognized in the IT community due to the pressure of meeting immediate production deadlines. Since September 11, 2001, passage of multiple legislation packages impacting the IT community, often indirectly, has occurred. The impact of these changes is still being determined by industry practitioners and the legal profession, with subsequent training activities required for full awareness and compliance by all affected groups. At a minimum, however, it is clear that security activities for information systems and assets will need to increase substantially to comply with these new regulations, or organizations will bear financial penalties and negligence legal determinations.
Related Content

Identifying Vulnerabilities of Advanced Persistent Threats: An Organizational Perspective
www.igi-global.com/article/identifying-vulnerabilities-of-advanced-persistent-threats/111283?camid=4v1a

Security Threats in the Internet of Things: RPL's Attacks and Countermeasures
www.igi-global.com/chapter/security-threats-in-the-internet-of-things/203786?camid=4v1a
Client-Side Detection of Clickjacking Attacks
www.igi-global.com/article/client-side-detection-of-clickjacking-attacks/145407?camid=4v1a

The Human Attack in Linguistic Steganography
www.igi-global.com/chapter/human-attack-linguistic-steganography/21353?camid=4v1a